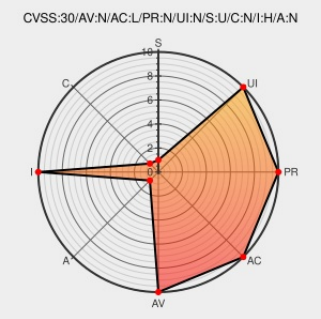
CVE-2018-20742

Published on: 01/24/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:36 PM UTC

CVE-2018-20742

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Opaque from Ucbrise contain the following vulnerability:

An issue was discovered in UC Berkeley RISE Opaque before 2018-12-01. There is no boundary check on ocall_malloc. The return value could be a pointer to enclave memory. It could cause an arbitrary enclave memory write.

CVE-2018-20742 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Security: No boundary check on `ocall_malloc` · Issue #66 · mc2-project/opaque · GitHub	Exploit, Patch, Third Party Advisory, github.com, text/html	MISC github.com/ucbrise/opaque/issues/66

Check that ecall [user_check] pointers and ocall_malloc result pointe… · mc2-project/opaque@5ddda15 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ucbrise/opaque/commit/5ddda15d89f5ac82f4416208c5319ace4aecdc36

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ucbrise	Opaque	All	All	All	All
Application	Ucbrise	Opaque	All	All	All	All

cpe:2.3:a:ucbrise:opaque:*:*:*:*:*:*:*:*:

cpe:2.3:a:ucbrise:opaque:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→